**Commonwealth of Massachusetts**

**Massachusetts Office of Information Technology - MassIT**

# Enterprise Access Control Policy

**Reference #: Ent-Pol-Sec-AccCtl-11.4.2 Issue Date: May 14, 2012
Issue #: Pri #17 Final v. 0.01**

## Table of Contents

[Table of Contents 1](#_Toc438198097)

[Executive Summary 1](#_Toc438198098)

[Whom this Policy Applies To 2](#_Toc438198099)

[Policy Statement 3](#_Toc438198100)

[Roles and Responsibilities 9](#_Toc438198101)

[Related Documents 11](#_Toc438198102)

[Contact 11](#_Toc438198103)

[Appendix A: Terms 12](#_Toc438198104)

[Appendix B: Document History 14](#_Toc438198105)

## Executive Summary

This policy articulates the access controls that are required to meet the security objectives of the [Enterprise Information Security Policy](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html). Access control management is paramount to protecting Commonwealth Information Technology (IT) Resources and requires implementation of controls and continuous oversight to restrict access.

Commonwealth Secretariats and their respective Agencies, authorities and business partners are required to protect applications, information assets, IT Resources and infrastructure against improper or unauthorized access which could result in compromise of confidentiality, integrity and availability of data and IT Resources.

This policy is organized into the following key sections which map directly to the ISO 27001/27002 Access Control Domain security objectives:

1. Business Requirements for Access Control
2. User Access Management
3. User Responsibilities
4. Network Access Control
5. Operating System Access Control
6. Application and Information Access Control
7. Mobile Computing and Teleworking

It is the responsibility of Agency Heads to have the appropriate combination of controls (administrative, technical, physical) in effect that provide reasonable assurance that security objectives are addressed. While an Agency Head may delegate this responsibility, the Agency Head remains accountable. Secretariats and their respective Agencies must achieve compliance with the overall information security goals of the Commonwealth, including compliance with laws, regulations, policies and standards to which their technology resources and data, including but not limited to personal information, are subject.

## Whom this Policy Applies To

All Secretariats and their respective Agencies and entities governed by the overarching [Enterprise Information Security Policy](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html)[[1]](#footnote-2) must adhere to requirements of this supporting policy as described below.

* Any entity that uses MassIT-controlled resources to access the Commonwealth's wide area network (MAGNet);
* Executive Department Secretariats and their respective Agencies, [[2]](#footnote-3) in addition to any agency or third party that connects to the Commonwealth’s wide area network (MAGNet), must comply with this policy.
* Executive Department Secretariats and their respective Agencies are required to ensure compliance by any business partner that accesses Executive Department IT Resources or shared environments, e.g. MAGNet;
* Executive Department Secretariats and their respective Agencies are required to ensure compliance by third parties in any aspect of the process of providing goods and services to their agency. These include, but are not limited to, electronic data collection, storage, processing, disposal, dissemination and maintenance. Third parties that interact in any way with Executive Department Commonwealth IT Resources, e.g. MAGNet, are required to comply with this policy; and
* Executive Department Secretariats, and their respective Agencies must develop and/or maintain an access control policy (including remote access) that documents Secretariats’ and their respective Agencies’ methodologies for providing access to authorized users either traditionally or remotely.

Other Commonwealth entities are encouraged to adopt, at a minimum, security requirements in accordance with this Enterprise Access Control Policy or a more stringent agency policy that addresses agency specific and business related directives, laws, and regulations.

## Policy Statement

The objective of this policy is to address the considerations that will help to ensure that the Commonwealth’s IT Resources and information assets are properly protected against unauthorized access, while meeting the access requirements for all authorized users. Critical to achieving this objective is the implementation of controls that address each of the requirements stated in this policy.

Executive Department Secretariats and their respective Agencies are required to implement necessary controls for providing authorized access and preventing unauthorized access to IT Resources and information assets on the basis of business, MGL, and security requirements.

### Business Requirements for Access Control

The objective of this requirement is to ensure that business, legal and security requirements drive the authorization process and access to IT Resources and information assets.

The following must be applied when evaluating the business requirements and implementing supporting access controls:

#### Access control policy:

Secretariats and respective Agencies must have a documented and periodically reviewed access control policy based on business and security requirements for access.

* + 1. Access to IT Resources and information must be commensurate with the security requirements of that resource and the classification of data it provides access to.
		2. Authentication methods used for accessing IT Resources and information must be consistent with the Security Controls articulated in the [Data Classification Standards](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/enterprise-information-security-standards.html)[[3]](#footnote-4).

### User Access Management:

The objective of implementing user access management is to ensure that authorized users are able to access information and resources while unauthorized users are prevented from access to the same.

#### User Registration

Secretariats and their respective Agencies must implement a formal user registration and de-registration procedure for granting and revoking access to all information resources and services.

#### Privilege Management

Access control rules must take into account existing policies for information dissemination and authorization while incorporating the principle of least privilege which grants the lowest level of access, rights, privileges, and security permissions needed for the performance of authorized tasks to any IT Resource or information.

Access Control rules must differentiate between different roles that may be applicable for an individual commensurate with the classification of the resources. For example, a general user who accesses information from a web site, the individual responsible for updating the content on a web site, the administrator of the application, and the network hosting administrator each have different roles that necessitate different privileges.

Acceptable implementation of this principle will include allocation of user privileges on a need-to-use basis, per system, per application, based on resource and data classification, business requirements, and job function.

#### User Password Management

Secretariats and their respective agencies must have a password policy and a formal process for password management and maintenance, along with a formal process to review the password policy and process periodically. The password policy, to the greatest extent technically feasible, should comply with NIST and FISMA standards, which specifically call for a password being comprised of at a minimum of eight characters, including capital and non-capital letters, numerical and special characters.

#### Review of User Access Rights

Secretariats and their respective Agencies must establish procedures and controls that cover all phases in the life-cycle of user access, authorization and privileges from provisioning to de-provisioning.

### User Responsibilities:

The objective of implementing user responsibility controls is to foster an informed and co-operative approach between users and the organization’s management for protecting IT Resources and data from unauthorized user access.

Executive Department Secretariats and their respective Agencies are required to obtain written user acknowledgement regarding the responsibilities associated with new access privileges prior to providing access credentials to the end user.

#### Password Use

Users are responsible for handling, use and storage of passwords in a manner that complies with all password management requirements noted in section 2. On addition:

#### Unattended User Equipment

Users are responsible for ensuring that unattended equipment has appropriate protection.

#### Clear desk and clear screen policy

Users are responsible for ensuring that information contained in papers and removable storage media on their desks, as well as information on their computer screens, has appropriate protection.

### Network Access Control:

The objective of Network Access Control is to provide access to internal and external networked systems in a controlled manner that is consistent with security policies.

Access to Commonwealth internal and external networked services via MAGNet must be protected through a combination of security controls including network segmentation, deployment of firewalls and other security appliances and appropriate authentication mechanisms to prevent and detect unauthorized access while providing secure access to authorized users and systems.

#### Policy on use of Network Services

Access to any given network service must only be granted to users who are specifically authorized to use that particular service.

#### User Authentication for External Connections:

Approved statewide remote access methods must be used for and by employees, contractors, contracted business partners, and statutory business partners.

#### Equipment Identification in Networks

Whenever possible, connections from specific locations and equipment must be authenticated using automatic equipment identification.

#### Remote Diagnostic and Configuration Port Protection

Any IT Resource that has a remote diagnostic or configuration service or facility must be evaluated to validate the need for remote access functionality.

#### Segregation in Networks

Secretariats and their respective Agencies must adopt a segmented approach to separate logical network domains.

#### Network Connection Control (flow control)

Users’ capability to connect to the Commonwealth shared network must be restricted according to access control policy and business application requirements.

#### Network Routing Control

Secretariats and their respective Agencies must implement network routing controls that enforce the network’s access control policies.

### Operating System Access Control:

The objective of implementing operating system access controls is to enable the ability to restrict access to operating systems to only authorized users.

Secretariats and their respective Agencies must have policies and procedures in effect to prevent unauthorized access to operating systems by employing controls that will properly authenticate users, provide appropriate access by role (e.g. Administrator), log activities, and generate notifications in the event of a breach.

#### Secure Log-on Procedures

Secretariats and their respective Agencies must adopt login procedures that minimize the opportunity for unauthorized access by implementing Security Controls.

#### User Identification and Authentication

Secretariats and their respective Agencies must ensure that User Identification and Authentication controls support the security objectives of the system or environment.

Secretariats and their respective Agencies must have procedures and controls in place that utilize authentication controls of strength commensurate with the sensitivity of the system and data accessible by authenticated users where appropriate, e.g. cryptographic means, smart cards, tokens or biometric means.

#### Password Management System

Secretariats and their respective Agencies must enforce policies and implement an effective password management system in accordance with the requirements of sections 2.3 and 3.1 of this policy.

#### Use of System Utilities

Secretariats and their respective Agencies must have system policies and procedures in place to tightly control access and permissions associated with utility programs including those that might be capable of overriding system and application controls.

In order to accomplish this, Secretariats and their respective Agencies must control the use of System Utilities using identification, authentication and authorization procedures.

#### Session Time-out

Secretariats and their respective Agencies must have system policies and procedures in place to shut down inactive sessions after a defined period of inactivity. Use of Session Time-out functionality must be consistent with the Security Controls articulated in the Session Time-out section of the Enterprise Access Control Standards.

#### Limitation of Connection Time

Secretariats and their respective Agencies must have system policies and procedures in place to limit connection time based on a defined period of inactivity. Use of connection time-based limitation functionality must be considered for systems and environments classified as having high sensitivity or high risk.

### Application and Information Access Control:

The objective of implementing application and information access control is to enable enforcement of access policies for information and system functions, protect against unauthorized access and prevent compromise of systems with which information resources are shared.

Secretariats and their respective Agencies must have policies and procedures in effect to prevent unauthorized access to application systems, application system functions, information contained within the applications and integrated sub-systems. Effective controls include use of layered security techniques, security controls, and standards to protect against compromise from any unauthorized access including but not limited to interactive users, applications, application services, etc.

#### Information Access Restriction

Secretariats and their respective Agencies must have access policies and procedures in effect to manage access to information and application system functions in accordance with both Enterprise and Secretariat and Agency policies. These policies and procedures must reflect the Enterprise Access Control Standards. All applications should follow current generally accepted control practices as promoted by respected security organizations including, but not limited to those published by The International Organization for Standardization (ISO), The National Institute of Standards & Technology (NIST), and The SysAdmin, Audit, Network, Security Institute (SANS), etc. Best practices such as these should form the basis of these policies and procedures.

#### Sensitive System Isolation

Secretariats and their respective Agencies must isolate systems containing data that is classified as having high sensitivity, e.g. FTI, PII, HIPAA, etc. Entities must have controls in effect to ensure that systems utilizing the public access architecture are properly secured and compliant with this policy and related standards. Entities need to ensure that appropriate monitoring mechanisms are in place to provide reasonable assurance that established controls are in effect. The isolated computing environment must protect an application system based on the explicitly identified and documented sensitivity classification and associated requirements as documented by the application owner. The isolated computing environment must also only be physically accessible to personnel that are approved such access by their respective Secretariat or Agency SCIO on an annually reviewed basis.

#### Logging and Monitoring

Secretariats and their respective Agencies must have system policies and procedures in place to address appropriate Logging and Monitoring functionality. Use of Logging and Monitoring functionality must be consistent with the Security Controls articulated in the Logging and Monitoring section of the Enterprise Access Control Standards.

#### Deployment and Maintenance

Secretariats and their respective Agencies must deploy and maintain application systems in a manner consistent with the Security Controls articulated in the Deployment and Maintenance section of the Enterprise Access Control Standards.

#### Application/Sub-Systems/Middleware

Secretariats and their respective Agencies who deploy applications using containers that provide execution environments distinct from the underlying operating system must employ controlled access to configuration and management functions provided by such environments with procedures and controls that are consistent with the Security Controls articulated in the Application/Sub-Systems/Middleware section of the Enterprise Access Control Standards.

### Mobile Computing and Teleworking:

The objective of implementing mobile computing and teleworking access controls is to protect against the unique risks introduced by accessing Commonwealth IT Resources from potentially unprotected environments.

Secretariats and their respective Agencies must have policies and procedures in effect to mitigate the additional risks by implementing security controls to protect IT Resources accessed from mobile or teleworking environments.

#### Mobile Computing and Communications:

Wireless and remote access methods and controls including Wireless Local Area Network (LAN) access (considered to be remote access) must use only approved and supported remote access methods and enforce required controls on Secretariat and Agency IT Resources. Users must sign all applicable Remote Access User Acknowledgments and/or Mobile Device Acknowledgments as required prior to being given access to any Commonwealth resources in a mobile fashion. Mobile devices must, to the greatest extent possible, adhere to the Password Management sections 2.3 and 3.1.

#### Teleworking:

In addition to complying with all of the requirements articulated in Section 4 of this policy, Secretariats and their respective Agencies must have policies and procedures in effect to mitigate and address added risks associated with Teleworking and remote access to IT Resources. Entities must adhere to Enterprise, Secretariat and Agency policies, standards, and contracts while accessing IT Resources via a teleworking environment, including but not limited to Acceptable Use Policy, VPN Policy, etc.

## Roles and Responsibilities

All Secretariats and their respective Agencies and entities governed by the overarching [Enterprise Information Security Policy](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html)[[4]](#footnote-5) are subject to the referenced roles and responsibilities in addition to those specifically stated within this supporting policy. The roles and responsibilities associated with implementation and compliance with this policy follow:

### Assistant Secretary for Information Technology

* Develop mandatory standards and procedures for Secretariats and their respective Agencies to follow before entering into contracts providing third parties with access to electronic high sensitivity information including, but not limited to, personal information or IT systems containing such information.
* Approval and adoption of this Enterprise Access Control Policy and its revisions.

### Secretariat Chief Information Officer (SCIO) and Agency Head

* Exercise due diligence in adhering to the requirements contained in this policy.
* Provide communication, training and enforcement of this policy that support the security goals of the Secretariat, its respective Agencies, and the Commonwealth.
* Provide proper third party oversight as applicable for access to and communication with agency IT Resources including applications and information assets.
* Ensure compliance with this policy for all prospective and actual wireless communications deployments, including vendor oversight.
* Ensure all wireless communications deployments in the state entity are sanctioned and supported by the entity’s information technology staff in compliance with this policy and related standards.

### Secretariat or Agency Information Security Officer (ISO)

* Ensure that the goals and requirements of the Enterprise Access Control Policy are met.

### Enterprise Security Board (ESB)

* Recommend revisions and updates to this policy and related standards.

### Massachusetts Office of Information Technology (MassIT)

* After review of any related recommendations of the Enterprise Security Board, issue revisions and updates to this policy and related standards.

### Third parties

* Ensure that all IT systems and applications developed by or for Executive Department agencies or operating within the Commonwealth’s Wide Area Network (MAGNet) conform to this and other applicable Enterprise Information Technology Policies, Standards and Procedures promulgated by the CIO. Non-conforming IT systems cannot be deployed unless the purchasing entity and their contractor have jointly applied for and received, in writing from the CIO or designee, notice that a specified deviation will be permitted.
* Comply with agency implementation of this policy at a minimum or a more stringent agency specific policy including:
	+ Attestation and certification that third parties have read [Executive Order 504](http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/legal-guidance/privacy-and-security/exec-order-504/)[[5]](#footnote-6) and this policy.
	+ Review and compliance with all information security programs, plans, guidelines, standards and policies that apply to work performed for their contracting agency.
	+ Communication of such provisions to and enforcement against their subcontractors, and implementation and maintenance of any other reasonable and appropriate security procedures and practices necessary to protect high sensitivity information, including but not limited to personal information, to which they are given access as part of the contract from unauthorized access, destruction, use, modification, disclosure or loss.

## Related Documents

Related Standards and Procedures include:

* Mass.Gov Portal
* Public Access Architecture
* Outlook Web Access (OWA) Procedures
* Security Shared Service Procedures
* VPN Procedures

Primary references that were used in development of this policy include:

* ISO 27001
* Executive Order 504

Additional information referenced includes:

* M.G.L., Ch 93H
* M.G.L., Ch 93I
* M.G.L., Ch 66A
* ISO 27002
* CobiT
* ITIL
* HIPAA Security Rule

## Contact

Standards@state.ma.us

## Appendix A: Terms

Key terms used in this policy have been provided below for your convenience. For a full list of terms please refer to the glossary of [Commonwealth Specific Terms](http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/glossary-of-commonwealth.html)[[6]](#footnote-7) on the Massachusetts Office of Information Technology’s website.

**Agency –** A department, bureau, commission, board, office, council, or other entity in the executive department of government, created by Massachusetts Constitution or statute.

**Business Partner –** A generic term referring to both contracted business partners and statutory business partners. (See definitions for “Contracted Business Partner” and “Statutory Business Partner” below).

**Contracted Business Partner –** An entity under contract with the Commonwealth with which the Commonwealth has an agreement to share data or engage in secure communications for a limited purpose. Contracted business partners do not include individuals who are under contract with and paid directly by the Commonwealth.

**Controlled Networks –** Networks physically or operationally controlled and security managed by a specific Commonwealth entity. Controls include physical, operating system, application, and patch security.

**Employees –** Agency’s employees or individuals under contract with the agency to provide services and paid directly by the agency whose work is controlled and directed by the agency.

**Hardware –** Computers and any physical equipment used in connection with them, such as keyboards, printers, etc.

**Information Technology (IT) Resources –** The Commonwealth’s computers, printers, and other peripherals, programs, local and wide area networks, access to the Internet when provided by the Commonwealth, and remote access methods including VPN.

**MAGNet –** Commonwealth’s Wide Area Computer Network.

**Outlook Web Access (OWA) –** A feature subset of Microsoft Outlook that allows MassMail users to remotely access their email via a web browser.

**Statutory Business Partner –** Individuals or entities that are not under contract with the Commonwealth and have a statutory right to access data held by the Commonwealth.

**User –** Any workforce member (or computer performing automated tasks) with a legitimate reason and purpose to use Commonwealth IT resources.

**Wireless Mobile Communications (WMC) –** WMC utilize licensed frequencies and include such services as 2G and 3G cellular telecommunications, Cellular Digital Packet Data (CDPD), Global System for Mobile Communication (GSM), and General Packet Radio Services (GPRS), among others. WWANs can span world-wide but are currently limited in data transmission rates, typically from 56Kbps to 300Kbps.

Wireless Wide Area Networks (WWAN, non-cellular) **–** High-speed point-to-point wireless connections, sometimes called Fixed Wireless to differentiate them from mobile wireless connections or Wireless LANs. For the purposes of this policy document, WWAN networks are defined as those utilizing FCC-licensed radio frequencies (microwave) for point-to-point communication between facilities. This section will only apply to client communication/use of devices that operate within FCC regulated frequencies, as unregulated frequency use is prohibited. Microwave networks support data communication rates from T1 to OC-3 – speeds are very dependent on the frequency, type of radio and protocol(s) utilized.

## Appendix B: Document History

| Date | Action | Effective Date | Next Review Date |
| --- | --- | --- | --- |
| 05/14/12 | Ref #11.4.2 Enterprise Access Control Policy published | 05/14/12 | 04/30/13 |
| 04/30/13 | Reviewed | 04/30/13 | 03/06/14 |
| 03/06/14 | Reviewed | 03/06/14 | 03/07/15 |
| 04/01/15 | Reviewed | 04/01/15 | 04/02/16 |
| 12/15/2015 | Accessibility remediation – no content changes | 2/22/15 | 1/1/17 |

1. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html [↑](#footnote-ref-2)
2. The Executive Department is comprised of the Executive Branch minus the Constitutional Offices, i.e., the State Auditor, State Treasurer, the Attorney General, and the Secretary of the Commonwealth. [↑](#footnote-ref-3)
3. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/enterprise-information-security-standards.html [↑](#footnote-ref-4)
4. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html [↑](#footnote-ref-5)
5. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/legal-guidance/privacy-and-security/exec-order-504/ [↑](#footnote-ref-6)
6. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/glossary-of-commonwealth.html [↑](#footnote-ref-7)